UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

FORTINET, INC.,

Plaintiff,

v.

FORESCOUT TECHNOLOGIES, INC.,

Defendant.

Case No. 20-cv-03343-EMC

ORDER ON MOTION FOR PARTIAL JUDGMENT ON THE PLEADINGS

Docket No. 208

I. INTRODUCTION

Forescout seeks partial judgment on the pleadings; it asserts that Fortinet's '662, '034, and '421 Patents are ineligible under 35 U.S.C. § 101 and *Alice Corp. Pty. Ltd v. CLS Bank International*, 573 U.S. 208, 216-17 (2014). These patents previously were analyzed for ineligibility at the motion to dismiss stage. Forescout re-asserts its ineligibility arguments in the instant motion for partial judgment on the pleadings. For the reasons stated below, Forescout's Motion for Partial Judgment on the Pleadings is GRANTED with respect to Claims 5 and 13 of Patent '662 and Claims 5 and 18 of Patent '421. However, Forescout's Motion is DENIED with respect to the remaining claims in Patents '662, '034, and '421.

II. BACKGROUND

A. Factual Background

Fortinet sells "cybersecurity products, software, and services" to large institutional customers. Compl. ¶ 3; *see also id.* ¶¶ 21-23. Many of Fortinet's product offerings specifically address "[t]he proliferation of [Internet of Things] devices," which "has made it necessary for organizations to improve their visibility into what is attached to their networks." *Id.* ¶ 25. The company's products thus "provide[] network visibility to see devices connected to a network as

well as the ability to control those devices and users." *Id.* ¶ 26. Fortinet is the owner, by assignment, of three patents relating to cybersecurity and network access control. These include United States Patent No. 9,948,662 ("Patent '662"), titled "Providing security in a communication network"; No. 9,894,034 ("Patent '034"), titled "Automated Configuration of Endpoint Security Management"; and No. 9,503,421 ("Patent '421"), titled "Security Information and Event Management." *Id.* ¶¶ 2, 30-39. Forescout is a competitor of Fortinet, also selling cybersecurity products to businesses. *See id.* ¶ 6.

B. Procedural Background

In its original complaint, Fortinet alleged infringement of several patents, including Patent '662, on theories of induced, contributory, and willful infringement. Compl. ¶¶ 37, 49, 51, 63, 65, 77. Forescout moved to dismiss for failure to state a claim, arguing primarily that Patent '662 was "directed to an abstract idea that lacks any inventive concept, and [is] therefore patent-ineligible" under 35 U.S.C. § 101. *See* Mot. to Dismiss, Docket No. 24. In its ruling, the Court declined to invalidate the Patent '662 on § 101 grounds. The Court agreed with Forescout that Patent '662 is directed to abstract ideas, Mot. to Dismiss Order at 10-12, 17-18, Docket No. 55, but was unable to conclude, at this early stage of the litigation, that the patents lacked an inventive concept, *id.* at 12-14, 18-19. While the Court expressed its skepticism about the ultimate validity of Patent '662 and stated that "the outcome of claim construction," in particular, "might make it appropriate . . . to revisit the eligibility questions" later in the proceedings, "such as at summary judgment," the Court could not conclude that the patent claimed ineligible subject matter on a motion to dismiss. *Id.* at 19.

Fortinet filed its First Amended Complaint ("FAC") in December 2020 asserting two additional patents: the '034 and '421 Patents. Forescout then moved to dismiss the FAC. The Court declined to invalidate the two newly asserted patents' claims under § 101. *See* Mot. to Dismiss FAC Order, Docket No. 94. With respect to Patent '034, the Court stated that the "'034 Patent appears, on its face, to be abstract," but that "other features of Patent '034 suggest that it may satisfy the step-one inquiry." *Id.* at 17-18. Based on some of the dependent claims and the specification, the Court concluded that "fact questions exists" as to whether the Claims are

"generic" and stated it "cannot conclude at this stage of the litigation that clear and convincing evidence proves this combination of claim elements to be 'well-understood, routine[,] and conventional to a skilled artisan in the relevant field." *Id*. at 19-20 (quoting *Berkheimer v. HP, Inc.*, 881 F.3d 1360, 1368 (Fed. Cir. 2018)). "The Court clarified that its ruling here is not prejudicial to Forescout's ability to renew its subject-matter-eligibility arguments at a later stage of the litigation, such as at summary judgment." *Id*. at 20. The Court reasserted that it remained "skeptical" of the ultimate validity of the patent. *Id*. With respect to Patent '421, the Court cited similar reasoning for denying Forescout's motion to dismiss. *See id*. at 25-26.

On November 28, 2022, the Court issued its claim construction order, discussed below. Forescout now moves for judgment on the pleadings.

III. LEGAL STANDARDS

A motion for judgment on the pleadings is proper "when the moving party clearly establishes on the face of the pleadings that no material issue of fact remains to be resolved and that it is entitled to judgment as a matter of law." *Hal Roach Studios, Inc. v. Richard Feiner and Co., Inc.*, 896 F.2d 1542, 1550 (9th Cir. 1989). In reviewing a motion under Rule 12(c), the court must assume that the facts alleged by the nonmoving party are true and must construe all inferences drawn from those facts in favor of the nonmoving party. "Rule 12(c) is 'functionally identical' to Rule 12(b)(6) and [ ] 'the same standard of review' applies to motions brought under either rule." *U.S. ex rel. Cafasso v. Gen. Dynamics C4 Sys., Inc.*, 637 F.3d 1047, 1054 n.4 (9th Cir. 2011) (citation omitted). Patent eligibility under § 101 is a threshold issue that courts may resolve on a Rule 12 motion "when there are no factual allegations that, taken as true, prevent resolving the eligibility question as a matter of law." *Voter Verified, Inc. v. Election Sys. & Software LLC*, 887 F.3d 1376, 1384 (Fed. Cir. 2018) (quotations omitted) (discussing Rule 12(b)(6).

IV. DISCUSSION

A. Procedural Propriety of Motion

Fortinet claims that this motion is procedurally improper because it is "a thinly-veiled (and unauthorized) motion for reconsideration." Opp'n at 4. The assertion is meritless. A motion

under Rule 12(c) may be brought after denial of a motion to dismiss under Rule 12(b). *See Preimesberger v. United States*, 541 F. Supp. 3d 1046, 1051 (E.D. Cal. 2021) (holding that a motion for judgment on the pleadings filed after a motion to dismiss was not an impermissibly filed motion for reconsideration). Courts have granted renewed § 101 motions under Rule 12(c) after a motion to dismiss and claim construction. *See, e.g.*, *Synopsys, Inc. v. Siemens Industry Software Inc.*, 2023 WL 5174291 (N.D. Cal. 2023) (district court considered moving party's motion for judgment on the pleadings after a motion to dismiss and claim construction), *appeal filed*, No-23-2440 (9th Cir. Sept. 29, 2023).[1] Here, the Court specifically indicated that the denial of the motion to dismiss was without prejudice to renewal.

B. Patent Eligible Subject Matter

In the Court's prior Orders, it detailed the patent ineligibility standards which are applicable in this context. Here, the Court relies on its prior legal analysis, and need not repeat itself. *See* Mot. to Dismiss Order, Docket No. 55; Mot. to Dismiss FAC Order, Docket No. 94.

C. Flexible Approach for Steps One and Two of the *Alice* Inquiry

For the reasons stated in its prior order, the Court adopts a flexible approach in "characteriz[ing] what the claims are directed to," taking both step-one and step-two considerations into account below. *See Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1339 (Fed. Cir. 2016).

D. The Role of the Specification

In the Court's prior Order, it discussed the specification's role in determining step one

[1] Fortinet cites two cases for its proposition that Forescout's motion should be denied, but neither are persuasive. In *Dekker v. Vivint Solar, Inc.*, the court declined to grant the moving party judgment on the pleadings because the motion asserted a motion for reconsideration—"explicitly contend[ing] that the court erred as a matter of law in the [prior] order and stat[ing] that it now 'renews' its [prior] motion." 542 F. Supp. 3d 959, 967 (N.D. Cal. 2021). The court did not suggest that any new facts were raised. *Id*. In another case, *Kimmel & Silverman, P.C. v. Porro*, the moving party sought judgment on the pleadings, "rely[ing] principally on the same arguments that they made in support of their motion to dismiss" which was "expressly addressed by the District Judge in his Order" and otherwise failing to "suggest that any new facts or law warrant reconsideration of this issue by the court." 969 F. Supp. 2d 46, 50 (Mass. 2013). There, the moving party's only new argument was "beside the point." *Id.*

eligibility. It stated:

> Given the Federal Circuit's ambiguous caselaw on the question of the specification's precise role at step one of the *Alice* test, as well as the level of detail the invention must provide in explaining how it functions, the Court believes it prudent, at this still-early stage of the litigation, to construe the focus of the '034 Patent "in light of the specification," *Enfish*, 822 F.3d at 1335, and to credit the specification's account of whether and how "the claimed invention achieves multiple technological improvements" over the prior art, *CardioNet*, 955 F.3d at 1368-69.

Motion to Dismiss FAC Order at 17, Docket No. 94. Forescout cites a new authority on this point. *See* Mot. 15. In *Hawk Tech. Sys., LLC v. Castle Retail, LLC*, the Federal Circuit stated that "the analysis at step one 'must focus on' the claim language." 60 F.4th 1349, 1358 (Fed. Cir. 2023) (quoting *ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 769 (Fed. Cir. 2019) ("Even a specification full of technical details about a physical invention may nonetheless conclude with claims that claim nothing more than the broad law or abstract idea underlying the claims.")). In *ChargePoint*, the Federal Circuit stated, "the specification cannot be used to import details from the specification if those details are not claimed." *Id*. While *Hawk Tech.* emphasizes the primacy of claims language, it does not overrule the Federal Circuit's prior authority on the relevance of the specifications as important intrinsic evidence that can inform claim construction. Therefore, the Court does not find *Hawk Tech.* warrants revision of this Court's prior analytical approach.

At the February 8, 2024, hearing, both parties agreed that the Court may address eligibility claim by claim, *i.e.*, the Court may find a specific claim to be patent ineligible. Indeed, as the Court previously discussed, at step two, if claims are directed to a patent-ineligible concept, "[courts] consider the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." *Alice*, 134 U.S. at 2355 (quoting *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 566 U.S. 66, 78-79 (2012)).

E. Patent Eligibility Analysis

1. Patent '662

Patent '662 is titled: "providing security in a communication network." According to its specification, Patent '662 relates to "methods and systems for providing security in a

communication network by selectively enabling various features for scanning user traffic streams." '662 Pat. at 1:16-20. The only remaining asserted claims are 5, 6, 13, and 14, which are all dependent claims. Mot. 6. Claims 5 and 6 depend on independent Claim 1 and Claims 13 and 14 depend on independent Claim 9. Patent '662, col. 14:53-16:40.

In the Court's Claim Construction Order, the Court construed the "trust level" of independent Claims 1 and 9 to mean "one of multiple (two or more) trust levels corresponding to the number of security features that can be disabled." Claim Construction Order at 51, Docket No. 174. The Court agreed with Forescout "that a 'trust level' must reflect more than a simply binary yes/no determination of whether a network is trusted." *Id.* at 52. The Court based this assertion on two points: (1) "a trust level is relevant for selecting security features only after an external network is determined to be trusted… [so] a trust level must encompass more than trust / not trusted determination"; and (2) "every reference to trust levels in the specification relates to multiple distinct trust levels." *Id*.

a. *Alice* Step One

The Court previously ruled on *Alice* step one in its first motion to dismiss Order, stating:

> At *Alice* step one, Forescout again argues that the patent is directed to "the abstract idea of controlling access," in this case by "using unspecified security features on a network based on simply analyzing data." Mot. at 13. Once more, it analogizes to *Prism* and *Dropbox*: as in the latter case, the claims here "recite the use of a 'trust level,'" which the court in the earlier case held insufficient to constitute a technological solution. *Id.* at 14 (citing *Dropbox*, 815 Fed. Appx. at 533). And as in *Dropbox*, the claims here fail to explain "how the 'selectively disabling' (or any other claim step) is accomplished." Mot. at 14. Fortinet responds that the '662 Patent is not abstract because it solves "the technical problem" that occurs when security features are deployed indiscriminately to out-of-network traffic streams. Opp'n at 11 (citing '662 Pat. at 1:16-51). The patent "solved this problem by selectively disabling and enabling security features on traffic streams based on the trust level of the destination," with the resulting benefit of "higher system performance" through "optimize[d] utilization of the system resources." *Id.* (citing '662 Pat. at 12:55-66). Fortinet analogizes to the claimed advances recently deemed patent-eligible by the Federal Circuit in *Packet Intelligence* and *SRI International v. Cisco Systems, Inc.* *See id.* at 11-12.
>
> Fortinet's analogies here are strained, as *Packet Intelligence* and *SRI* are firmly focused on the particularities of computer-network

> technology.[2] With the '662 Patent, in contrast, it is easy to generalize the claimed advance as a far broader "method of organizing human activity." *See Alice*, 573 U.S. at 220. As Forescout notes, "[r]elaxing security measures for trusted users is an abstract and longstanding human activity, no different than waiving x-ray checkpoints for pilots and flight attendants." Reply at 5; *see also Dropbox*, 815 Fed. Appx. at 532 (denying eligibility to "a nearly identical system for controlling access that 'provide[s] the resource only if the trust level for the mode of identification is sufficient for the sensitivity level of the resource'"). Forescout also makes the sensible point that the benefits to system performance claimed by Fortinet are merely incidental to "*not* limiting access" and do not flow—as they must at step one—from "an improvement in the functionality of the . . . network platform itself." Reply at 6 (quoting *Customedia*, 951 F.3d at 1364). The '662 Patent is therefore directed to "the abstract idea of disabling security for trusted communication," *id.*, reciting ineligible subject matter at *Alice* step one.

Mot. to Dismiss Order at 17-18, Docket No. 55. Thus, Patent '662 is directed to an abstract idea.[3]

b. *Alice* Step Two

In the Court's motion to dismiss Order, it stated:

> Proceeding to *Alice* step two, Forescout emphasizes that the patent neither "require[s] any special hardware . . . nor does [it] disclose any novel hardware"; instead, the hardware that it mentions "is conventional and described in highly generic and functional terms." Mot. at 19. Indeed, Forescout shows that the specification identifies many well-known "network security devices" (e.g., "network firewalling, VPN, antivirus," etc.), "teaches the use of known client computing devices" (e.g., "fax machines, printers, scanners," etc.), and "further identifies multiple known network types for use in the invention" (e.g., "direct connect, Ethernet," etc.). *Id*. at 19-20 (quoting '662 Pat. at 4:6-12, 5:13-20, 5:24-35). "The patent also admits that security features [recited in the claims] were known in 'conventional methods and systems.'" *Id*. at 20 (quoting '662 Pat. at 1:39-51).
>
> As with the '299 Patent, Fortinet argues that the inventive concept of the '662 Patent is the very idea to which it was directed at step

---

[2] In *Packet Intelligence*, the court held that a claim "solve[d] a technological problem" "unique to computer networks," *i.e.*, "identifying disjointed connection flows in a network environment" to provide more "granular, nuanced, and useful classifications of network traffic." 965 F.3d at 1309-10. And in *SRI*, the court held that "using a plurality of network monitors" and "integrating reports from the monitors" solved a specifically "technological problem arising in computer networks: identifying hackers or potential intruders into the network." 930 F.3d at 1303.

[3] Despite the Court's prior ruling, Fortinet maintains that the claims of the '662 Patent are not directed to an abstract idea because they recite a technological solution to a technological problem—determining *what* communications are to be trusted. *See* Opp'n at 5. However, the Court need not reconstrue its prior order at this juncture.

one, i.e., "selectively disabling a subset of security features upon a determination that an external network is trusted." Opp'n at 17. But if the focus of the claim is found to be a patent-ineligible abstract idea then that same idea cannot also constitute an inventive concept at step two. *See Chamberlain Grp., Inc. v. Techtronic Indus. Co.*, 935 F.3d 1341, 1349 (Fed. Cir. 2019) (confirming that "the abstract idea that the claims are directed to" "cannot be an inventive concept"). Beyond this contention, Fortinet offers only the conclusory and "boilerplate" statement that "the ordered combination of the recited limitations is not generic and was neither routine nor conventional at the time of invention." Reply at 9; Opp'n at 17.

But Fortinet also contends that dependent claims 7, 9, and 15 "further limit and explain the content and structure of the step of receiving a trust identifier" and that the specification "describes how the specific claimed methods address shortcomings in 'conventional methods and systems.'" Opp'n at 17 (quoting '662 Pat. at 1:39-51, 1:55-58).[4] While these allegations are perhaps little more than the boilerplate Fortinet elsewhere offers in arguing for the inventiveness of the '662 Patent, it again points out that these issues represent "exactly the type of fact question" that cannot be resolved on the pleadings. *See id*. (citing *Berkheimer*, 881 F.3d at 1368). Forescout makes the colorable argument that, in this case, the Court need only look "to the specification, which describes the [components] as

---

[4] Claims 7 and 15 are substantially similar. Claim 9 is an independent claim. Claims 7 and 9 are as follows:

Claim 7 (which is no longer asserted):
The method of claim 6, further comprising receiving, by the network security device, a trust identifier from the trusted network parameters database when a domain or a URL of the application protocol request corresponds to a trusted IP address.

Claim 9 (which is no longer asserted):
A network security device comprising:
At least one processor; and
A computer-readable medium storing instructions that, when executed by the at least one processor, cause the at least one processor to perform a method comprising:

Receiving an application protocol request directed to an external network that is originated by a client device associated with an enterprise network protected by the network security device;

Determining based on the application protocol request whether a network parameter of the external network is associated with a set of trusted networks; and

Selectively disabling application of a subset of security features of a plurality of security features to be applied to network traffic exchanged between the client device and the external network while the client device is accessing the external network when a result of said determining is affirmative, wherein the subset of security features are selected based on a trust level associated with the external network.

> either performing basic computer functions . . . or performing functions 'known' in the art." *In re TLI Commc'ns*, 823 F.3d at 613-14. This discussion underscores the potential value of claim construction and development of facts that may inform the § 101 analysis.

Mot. to Dismiss Order at 18-19, Docket No. 55. The Court concluded:

> As the foregoing indicates, the Court remains skeptical of the subject-matter eligibility of Fortinet's asserted patents (especially the '662 Patent). But it cannot, at this juncture, hold that the '662 Patent invalid under § 101. This decision not to dismiss does not preclude Forescout from re-raising the § 101 issue at a later stage of litigation, such as at summary judgment. In fact, at the hearing on Forescout's motion to dismiss, counsel for Fortinet agreed that the outcome of claim construction might make it appropriate for the Court to revisit the eligibility questions addressed above. Docket No. 45 ("Tr.") at 22.

Id. at 19.

In the Court's prior Order, it discussed Claims 7, 9, and 15 as essentially saving Patent '662 from ineligibility at *Alice* step two. However, those claims are no longer asserted. Thus, the question is whether the remaining claims, Claims 5, 6, 13, and 14, "limit and explain the content and structure of the step of receiving a trust identifier," as the Court found with Claims 7, 9, and 15. *See* Mot. to Dismiss Order, Docket No. 55 at 19.

a. Claims 5 and 13

Claim 1, which is no longer asserted, essentially lays out a method for a network security device to (1) receive a request to join the network, (2) determine whether the external network is trustworthy, and (3) selectively disable the network's security features in accordance with the trustworthiness of the external network. *See* Patent '662, Claim 1. In particular, Claim 1 sets forth:

> A method comprising:
>
> Receiving, by a network security device within an enterprise network, an application protocol request directed to an external network that is originated by a client device associated with the enterprise network;
>
> Determining, by the network security device, based on the application protocol request whether a network parameter of the external network is associated with a set of trusted networks; and
>
> Selectively disabling, by the network security device, application of a subset of security features of a plurality of security features to be applied to network traffic

> exchanged between the client device and the external network while the client device is accessing the external network when a result of said determining is affirmative, wherein the subset of security features are selected based on a trust level associated with the external network.

Patent '662, Claim 1. Claim 5, which is substantially similar to Claim 13, and is still asserted, recites:

> The method of claim 1, wherein the network parameter is selected from a group comprising a domain, a Uniform Resource Locator (URL), a destination Internet Protocol (IP) address, a port number, a protocol and a service.

Patent '662, Claim 5. Claim 13 states:

> The network security device of claim 9, wherein the network parameter is selected from a group comprising a domain, a Uniform Resource Locator (URL), a destination Internet Protocol (IP) address, a port number, a protocol and a service.

Patent '662, Claim 13. This language merely "enumerat[es] types of information and information sources … for collection, analysis, and display [which] does nothing significant to differentiate a process from ordinary mental process." *Elec. Power Grp. v. Alstom S.A.*, 830 F.3d 1350, 1355 (Fed. Cir. 2016). This claim does not shed light on *how* Patent '662 selectively disables or enables security features; it does not suggest "an inventive concept in the non-abstract application realm." *SAP America, Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1169 (Fed. Cir. 2018). It simply displays several generic devices from which the network parameter selects. *See Weisner v. Google LLC*, 51 F.4th 1073, 1084 (Fed. Cir. 2022) ("these claims do not recite significantly more than the abstract idea of digitizing a travel log using conventional components"; citing claim language describing methods to "receive and transmit wirelessly" including "methods such as Bluetooth"). It says nothing about how the network parameter makes selections. Thus, Claims 5 and 13 provide no inventive value and are patent ineligible.

b. Claims 6 and 14

Claim 6, which is substantially similar to claim 14, and is still asserted, recites:

> The method of claim 5, wherein said determining comprises querying, by the network security device, a trusted network parameters database including a list of trusted network parameters

> associated with the set of trusted networks.

Patent '662, Claim 6. Claim 14 states:

> The network security device of claim 13, wherein said determining comprises querying a trusted network parameters database including a list of trusted network parameters associated with the set of trusted networks.

Patent '662, Claim 14. Thus, Claims 6 and 14 are directed to the second step of determining wherein the network security device queries its database to determine the trustworthiness level, and the database includes a list of trusted network parameters.

Fortinet argues that Patent '662 "claims a specific technique for *how* to determine whether network traffic is trusted, by analyzing the network parameters associated with application protocol requests specifically" and it "recites specialized software to carry out this specific technique." Opp'n at 8. Fortinet states that Claims 6 and 14 "expand on this *how* aspect even further, reciting a database of network parameters, an unconventional use of a database." *Id*. at 10. Fortinet cites *BASCOM Global Internet Services, Inc. v. AT&T Mobility LLC*, where after a corporation developed a software tool to "provide individually customizable filtering at the [Internet] server by taking advantage of the technical capability of certain communication networks" to filter content, like "entertainment oriented sites," the Federal Circuit deemed the patent to be a non-abstract invention. 827 F.3d 1341, 1345 (Fed. Cir. 2016). Though the limitations of the claims recited generic computer components, and "filtering content on the internet was already a known concept," "the patent describe[d] how its particular arrangement of elements [was] a technical improvement over prior art ways of filtering such content." *Id*. at 1350. Likewise, Fortinet argues Patent '662 has "the idea of analyzing a specific kind of network traffic (application protocol requests) in a specific way (looking at their network parameters) to deploy specific kinds of security features, by a specific kind of device (a network security device) deployed on an enterprise network," which is not abstract or generic. Opp'n at 9.

Forescout counters stating that *BASCOM* is inapplicable because the filtering tool described in *BASCOM* improved the performance of the computer itself, and Patent '662 does not improve the computer's performance. However, Patent '662's specification states: "when a

trusted network is being accessed, selectively disabling some of the security features optimizes the utilization of system resources in order to gain higher performance." Patent '662, col. 7:59-62.

Forescout also argues that Claim 6 and 14's use of a database or a list of trusted network parameters is not conventional. Reply at 7. However, Claims 6 and 14 state that the network security device queries a trusted network parameters database and that the database includes a list of trusted network parameters associated with the set of trusted networks. Though it is not clear what "associated with" means at this juncture, the specification states that one of the ways a trust level may be assigned is from "data available" which "may include the number of times an external network has been accessed by online users, the numbers of times an external network has been flagged as a security threat, and the number of users who have blocked an external network." Patent '662, col. 8:41-47. Indeed, in the Court's prior Order, it stated that there remains a fact question as to whether the specification "describes how the specific claimed methods address shortcomings in 'conventional methods and systems'" or it "describes … performing functions 'known' in the art," as argued by Fortinet and Forescout, respectively. Mot. to Dismiss Order, Docket No. 55, 19. The Court stated this was "exactly the type of fact question" that cannot be resolved on the pleadings. *Berkheimer*, 881 F.3d at 1368.

Fortinet further points out that, in the Court's Claim Construction Order, the Court held that "trust level" had multiple levels which "correspond[s] to the number of security features that can be disabled." Claim Construction Order at 51, Docket No. 174. Forescout argues that this represents a "longstanding human practice"—similar to the "x-ray checkpoint" at airports analogy the Court previously adopted at step one. There, the Court stated "as Forescout notes, '[r]elaxing security measures for trusted users is an abstract and longstanding human activity, no different than waiving x-ray checkpoints for pilots and flight attendants.'" Mot. to Dismiss Order at 18, Docket No. 55. Forescout contends that "X-ray checkpoints" at airports involve a range of trust levels like (1) general boarding, (2) bypassing physical screening for passengers who have TSA PreCheck, (3) bypassing certain document checks for passengers who have CLEAR, and (4) bypassing both for passengers who have TSA PreCheck and CLEAR. *See* Mot. 10-11. Fortinet counters stating that this analogy is not persuasive, because the travelers with TSA PreCheck self-

identify whereas Patent '662 "import[s] the specific method … for discerning trust." Opp'n 10. Fortinet's distinction is persuasive—the Patent is more than a "method of organizing human activity," *Alice*, 573 U.S. at 220, because it purports to "query" a database of "trusted network parameters [that are] associated with a set of trusted networks." Claim 6. In other words, Claims 6 and 14's methods are eligible because their methods are distinguishable from the TSA analogy which describes an ineligible process.

Finally, in the parties' papers, they dispute whether Patent '662 contains generic terms, whether "the claims [or] the specification call for any parallel processing architectures different from those available in existing systems," *SAP*, 898 F.3d at 1170, and whether Patent '662 performs functions "known" in the art. Here, the parties do not address whether the Court has sufficient information to make a determination about whether the specification describes "base computer functions" or functions "known in the art." That is why the Court had previously deferred ruling on the eligibility of Patent '662 until the parties could develop expert testimony on these issues. At this juncture, the Court declines to find Claims 6 and 14 patent ineligible.

2. Patent '034

Patent '034 is titled "Automated Configuration of Endpoint Security Management." Patent '034 concerns "[s]ystems and methods for managing configuration of a client security application based on a network environment in which the client device is operating." Compl. ¶ 37 (quoting Patent '034 at Abstract). "In other words, the alleged invention selects the 'configuration' for a security application based on a device's condition, *i.e.*, its 'network environment.'" Mot. 12. Presently, there are only three asserted dependent Claims: 4, 9, and 23. Mot. 12. Each of these claims is dependent on independent Claim 1. *See* Patent '034. In the Court's prior order, it described this patent as follows:

> According to the patent's specification, "it is a challenge in network security management to keep a network secure while allowing many different devices to connect to the network." Compl. ¶ 37 (citing '034 Patent at 1:23-25). One way that user devices can connect to a network remotely is through a client security application, which must be configured "based on information regarding the network environment in which the user device is operating." *Id.* (citing '034 Patent at 1:50-54). The inventors of the '034 Patent solved the aforementioned security challenge "by having the client security

> application [1] determine [the user device's] network connection state with respect to a private network, [2] select a configuration based on this, and [3] launch functionality" (*e.g.*, "web content filtering, anti-virus scanning, and network access logging") "based on the [the application's] determination and selected configuration." *Id*. (citing '034 Patent at 1:56-60) (bracketed numbers added). The invention purportedly represents an advance over the prior art, which "typically required users to change the configuration of their device manually when changing networks or access methods in order for the corresponding functions of the client security application to be launched." *Id*. (citing '034 Patent at 1:44-50). The Amended Complaint states that the patent "solved this problem in a non-conventional way" and that the "ordered combination of the claimed steps is not generic and was neither routine nor conventional at the time of invention." *Id.*

Mot. to Dismiss FAC Order at 10-11, Docket No. 94. For Patent '034, the parties asked the Court to construe two terms: (1) "initialization of a client security application" in Claim 1; and (2) "initialization of the endpoint security application" in Claim 15. Claim Construction Order at 53, Docket No. 174. In particular, the parties' dispute centered on the word "initialization." *Id*. at 54. The Court construed both terms as consistent with their "plain and ordinary meaning." *Id*. at 53. Initialization "describes the preparation of the client security application to perform its tasks," consistent with its dictionary definition, "prepar[ation] of hardware or software to perform a task." *Id*. at 54-55.

a. *Alice* Step One

In the Court's motion to dismiss the FAC Order, with respect to Patent '034, it stated:

> The Court nevertheless agrees with Forescout that Claim 1 of the '034 Patent appears, on its face, to be abstract. According to Claim 1, the method entails a client security application enabling a client device (1) to "determin[e]" its "network connection state," (2) to "select[] . . . a configuration for the client security application" based on this network connection state, and (3) to "launch[] . . . one or more" predetermined "functions of the client security application," including "web content filtering, anti-virus scanning, [or] network access logging." *See*'034 Patent at Clm. 1. As Forescout argues, this relatively simple three-step process seems directed to little more than "the abstract idea of making a selection based on a condition." Docket No. 74 ("Reply") at 1. The claim language also lacks the kind of technological specificity concerning how the invention's desired result (*i.e.*, improved endpoint security management) is achieved that the Federal Circuit has oftentimes required to satisfy step one. *See, e.g.*, *Dropbox*, 815 Fed. Appx. at 532-33; *Ericsson*, 955 F.3d at 1326 (holding an invention abstract at step one where, *inter alia*, it did "not specify how the claim" achieved its desired result). Restricted solely to the language of

> Claim 1, therefore, the Court would have little trouble concluding that the '034 Patent recites ineligible subject matter at *Alice* step one.[5]
>
> As Fortinet contends, however, other features of the '034 Patent suggest that it may satisfy the step-one inquiry, at least in light of cases such as *CardioNet* and *Visual Memory*. First, several dependent claims refer to specific technological features that plausibly restrict the invention to the realm of the technologically concrete rather than the abstract. Claim 5, for example, comprises a limitation of dependent Claim 3, and entails a "Dynamic Host Configuration Protocol (DHCP) client of the client device" sending a "DHCP packet to a network appliance" and then "receiving . . . an acknowledgment DHCP packet" that contains the appliance's "identification information." '034 Patent at Clm. 5. Claim 8 then further limits Claim 5 so that the aforementioned functions "include one or more of Secure Sockets Layer (SSL)/Internet Protocol Security Protocol (IPSec) Virtual Private Networking (VPN), application firewalling, two-factor authentication, vulnerability scanning and Wide Area Network (WAN) optimization." *Id.* at Clm. 8.[6] While Forescout insists that such features are merely

---

[5] Claim 5:
A method comprising:
During initialization of a client security application running on a client device:

Determining, by the client security application, a network connection state of the client device with respect to a private network;

Selecting, by the client security application, a configuration for the client security application based on the determined network connection state; and

Launching, by the client security application, one or more functions of the client security application that are designated by the selected configuration to be performed by the client security application, wherein the one or more functions include one or more of web content filtering, anti-virus scanning and network access logging.

[6] Claim 3:
The method of claim 2, wherein said determining whether the client device is connected indirectly to the private network via an intermediate public network comprises determining, by the client security application, presence of identification information stored on the client device that is associated with one or more network appliances that are protecting the private network.

Claim 5:
The method claim 3, further comprising: sending, by a Dynamic Host Configuration Protocol (DHCP) client of the client device, a DHCP packet to a network appliance of the one or more network appliances; and responsive to the DHCP packet, receiving by the DHCP client, an acknowledgement DHCP packet containing therein the identification information.

Claim 8:
The method of claim 5, wherein the one or more functions further include one or more of Secure Sockets Layer (SSL)/Internet Protocol Security Protocol (IPSec) Virtual Private Networking (VPN), application firewalling, two-factor

> "conventional," Reply at 4, the Court is unable to deduce as much from the claims themselves or the specification. Rather, these dependent-claim limitations seem to "further specif[y] the physical features or operations" of the patented device, suggesting that it is directed to something that is technologically concrete. *See CardioNet*, 955 F.3d at 1369.
>
> Additionally, the '034 Patent's specification provides reasonably detailed explanations of how the invention functions in preferred embodiments and suggests "that the claimed invention achieves [multiple] benefits over conventional" technology in the field. *See Enfish*, 822 F.3d at 1337. Describing Figure 5, for instance, the specification explains that "[a]fter the appropriate configuration is selected based on the client device's network environment state … the client security application continues the startup procedure by launching the functions/engines that are associated with the corresponding configuration." '034 Patent at 8:55-59. The specification then provides a more detailed example of how the startup procedure works: "[W]hen an off-net configuration is selected and SSL/IPsec VPN and web filtering are enabled . . . the client security application launches a VPN dial-up module and establishes a VPN connection with a gateway of a private network using predefined VPN parameters." *Id.* at 8:59-65. Based on details like these in the specification, it may be argued that the'034 Patent is "more effective at securing large computer networks when automatically deployed at scale across an entire network," and that the manual version of patent's security tasks "reduc[es] the security of the entire network by limiting compliance with security protocols to that provided by human users." *See id.* at 6-7 (citing '034 Patent at 1:35-54). Absent further developments in this case (*e.g.*, claim construction or expert testimony), the Court is reluctant to reach a conclusion at this stage as to whether "the claimed invention achieves multiple technological improvements" over the prior art. *See CardioNet*, 955 F.3d at 1368-69.

Mot. to Dismiss FAC Order at 17-19, Docket No. 94.

b. *Alice* Step Two

In the Court's second Motion to Dismiss Order, it continued its discussion of Patent '034 with respect to *Alice* step two:

> Nevertheless, even if the Court were to find the '034 Patent directed to ineligible subject matter at step one, it would be hard pressed to reach the same conclusion at step two—recognizing, again, that "an analysis of whether there are arguably concrete improvements in the recited computer technology could take place under" either step one or step two. *See Enfish*, 822 F.3d at 1339. The step-two inquiry, as stated above, focuses on whether the claims contain an "inventive concept," i.e., "a claim element or combination of elements" that goes beyond that which is "well-understood, routine[,] and

---

authentication, vulnerability scanning and Wide Area Network (WAN) optimization.

> conventional to a skilled artisan in the relevant field." *Berkheimer*, 881 F.3d at 1368.
>
> Here, Fortinet plausibly argues that "fact questions exist as to whether the limitations of at least Claims [1 and 5] contain features, either individually or in an ordered combination, that are non-generic, not well understood, and not well known." Opp'n at 15. Claim 5, as noted above, involves "sending, by a [DHCP] client of the client device, a DHCP packet to a network appliance of the one or more network appliances," and then "receiving[,] by the DHCP client, an acknowledgement DHCP packet containing . . . identification information." '034 Patent at Clm. 5. Similarly, Claim 14 recites identification information that "comprises (i) a serial number or a hash value of the serial number of the one or more network appliances, (ii) a unique name of the one or more network appliances or (iii) a hash value of a plurality of serial numbers of the one or more network appliances." *Id.* at Clm. 14. Again, the Court cannot conclude at this stage of the litigation that clear and convincing evidence proves this combination of claim elements to be "well-understood, routine[,] and conventional to a skilled artisan in the relevant field." *See Berkheimer*, 881 F.3d at 1368.
>
> The Court therefore declines, at this time, to hold the '034 Patent invalid on the grounds of § 101, whether viewed in light of the step-one or step-two analyses, or as a consolidation thereof. The Court clarifies that its ruling here is not prejudicial to Forescout's ability to renew its subject-matter-eligibility arguments at a later stage of the litigation, such as at summary judgment. The Court also observes that, as with the '314, '299, and '662 Patents, it remains skeptical of the ultimate validity of '034 Patent, especially given Fortinet's failure, to this point, to articulate meaningful differences between the patent's independent and dependent claims. For now, however, the Court DENIES Forescout's motion to dismiss on the grounds that the '034 Patent claims ineligible subject matter.

Mot. to Dismiss FAC Order at 19-20, Docket No. 94.

c. Claim 4

Claim 1 is no longer asserted, but it is the independent claim on which Claim 4 depends. The invention in Claim 1 is described as follows:

> A method comprising:
>
> During initialization of a client security application running on a client device:
>
> Determining, by the client security application, a network connection state of the client device with respect to a private network;
>
> Selecting, by the client security application, a configuration for the client security application based on the determined network connection state; and

> Launching, by the client security application, one or more functions of the client security application that are designated by the selected configuration to be performed by the client security application, wherein the one or more functions include one or more of web content filtering, anti-virus scanning and network access logging.

Patent '034, Claim 1. This process ensures the safety of all devices connected to a "bring your own device" secure network. Claim 4 builds on non-asserted Claims 2 and 3, which all pertain to the second step of selecting a configuration. Claim 2, which is no longer asserted, recites:

> The method of claim 1, wherein said determining a network connection state of the client device with respect to a private network comprises determining whether the client device is connected indirectly to the private network via an intermediate network.

Patent '034, Claim 2. Claim 3, which is no longer asserted, recites:

> The method of claim 2, wherein said determining whether the client device is connected indirectly to the private network via an intermediate public network comprises determining, by the client security application, presence of identification information stored on the client device that is associated with one or more network appliances that are protecting the private network.

Patent '034, Claim 3. Claim 4 is still asserted and states:

> The method of claim 3, wherein said determining whether the client device is connected indirectly to the private network via an intermediate public network further comprises determining, by the client security application, whether the identification information matches previously stored identification information associated with a network appliance with which the client security application is registered.

Patent '034, Claim 4.

At *Alice* step one, there are questions as to whether Claim 4 is abstract on its face. The Court had previously found that Claim 1 was abstract on its face and Claim 4 merely adds an intermediary step to the "determining" function of Claim 1. In Claim 4's intermediary step, the client security application determines "whether the identification information matches previously stored identification information associated with a network appliance with which the client security application is registered." Patent '034, Claim 4. This is similar to "comparing the content-based identifier against other values," which the Federal Circuit held to be abstract in

PersonalWeb, 8 F.4th at 1316-17 (the Court likened the claims to "the 'abstract idea of (1) collecting data [and] (2) recognizing certain data within the collected data set.'"). Additionally, the claim language also lacks the kind of technological specificity concerning how the invention's desired result (*i.e.*, improved endpoint security management) is achieved that the Federal Circuit has oftentimes required to satisfy step one. *See, e.g.*, *Dropbox, Inc. v. Synchronoss Technologies, Inc.*, 815 Fed. Appx. 529, 532-33 (Fed. Cir. 2020); *Ericsson, Inc. v. TCL Commc'n Tech. Holdings Ltd.*, 955 F.3d 1317, 1326 (Fed. Cir. 2020) (holding an invention abstract at step one where, *inter alia*, it did "not specify how the claim" achieved its desired result).

Forescout asserts that, since the Court's ruling, the Federal Circuit has reaffirmed that providing information based on meeting a condition is abstract in *Sanderling Mgmt. Ltd. v. Snap Inc.*, 65 F.4th 698 (Fed. Cir. 2023), at the motion to dismiss stage. In *Sanderling*, the claim at issue represented a "computerized method of distributing a digital image processing function" to "load digital image branding functions to users when certain conditions are met." *Id.* at 701. The method used a server to access a database storing at least one digital image processing function "receiving … a Global Positioning System (GPS) location indication from each of a plurality of mobile devices … [and] matching … each said GPS location indication with said geographic location; and automatically forwarding … at least one digital image processing function to at least one mobile device … to create an output digital image." *Id.* Addressing *Alice* step one, the court stated: "The claims of the asserted patents are not directed to a specific improvement in computer functionality but, instead, to the use of computers as a tool." *Id.* at 703. This patent merely received, matched, and distributed information, and distribution is an abstract idea. *See id.* Fortinet disputes that *Sanderling* is applicable here. Fortinet states that the *Sanderling* claims used the computers as mere tools to distribute information of a particular variety, but that the claims were not directed to a specific improvement in computer functionality as here. *See* Opp'n 13. Fortinet states that, by contrast, the "network connection state" is not generic, rather, it improves the functionality of the network through its determination.

The Court is not persuaded that Claim 4 is less abstract than the claim in *Sanderling*. Nonetheless, the Court is unable to conclude that Claim 4 is patent ineligible at this juncture.

Forescout contends that Claim 4 merely requires "checking to see if one set of information matches another set of information [which] is not a technological advance, but a longstanding activity that humans routinely perform, both mentally and on paper." Mot. 16. In response, Fortinet states that whether a claim could be performed by a human does not render it abstract. *See* Opp'n 14. Fortinet contends that prior to this invention, the user or a technician determined which functionality is required based on understanding the needs of the network. *See id*. The devices would have either needed constant, human error-prone reconfiguration, by trained administrators, or to be fixed in place in desks at offices where they needed no reconfiguration but were not suited to the modern day of working in multiple locations. *See id*. This patent provides a convenient, flexible way to manage the security of the devices based on the network environment. Fortinet likens this to *McRO, Inc. v. Bandai Namco Games America Inc.*, 837 F.3d 1299 (Fed. Cir. 2016). There, the patents "relate[d] to automating part of a preexisting 3-D animation method" of animating 3-D characters faces and facial expressions while characters speak. *Id*. at 1303. Though humans are capable of creating 3-D animation on computers, "it [was] the incorporation of the claimed rules, not the use of the computer, that 'improved [the] existing technological process' by allowing the automation of further tasks." *Id*. at 1314 (citations omitted). Forescout responds stating that *McRO* is distinguishable because the patent there employed different rules and processes that the humans were not previously employing. Reply at 11. However, here, the specification illustrates that there is at least a factual dispute as to whether the system improves human processes by innovating technological procedures:

> [T]he client security application may compare the retrieved identification information with the identification information of one or more network appliances with which the client security application is registered. It will be apparent to one skilled in the art that it is possible that the on-net state may be determined if identification information is simply available on the client device; however, by comparing the retrieved identification information with the registered identification information, the client security application may determine that the client device is within a network that is controlled by a firewall with which the client security application is registered. If the retrieved identification information matches with the registered identification information, the client security application may determine that the client device is on-net and the process continues with block 504 [referring to fig. 5]. If the

> retrieved identification information does not match the registered identification information or there is no identification information is retrievable/available, the client security application may determine that the client device is off-net and the process branches to block 505.
>
> At block 504, it has been determined that the client device is an on-net network environment state. As such, the client security application selects an on-net configuration. The on-net configuration may be the default on-net configuration that is received by the client security application when registered with the network appliance. The user of the client security application may also setup or change the on-net configuration.

Patent '034, col. 8:20-48.

Furthermore, Fortinet states that Patent '034 discusses how the devices "determine" the "network connection state." Opp'n 13. Specifically, Fortinet states that Claim 4 presents this detail because it "recite[s] aspects of how this network connection state is determined—by, *e.g.*, having the security application communicate with a network appliance to receive identification information that it can use to figure out if there is an intermediary public network between it and the private network to which it is connected." Opp'n at 14. Again, the Court cannot conclude at this stage of the litigation that clear and convincing evidence proves this claim element is "well-understood, routine[,] and conventional to a skilled artisan in the relevant field." *Berkheimer*, 881 F.3d at 1368. Thus, Claim 4 survives this stage in the litigation.

d. Claims 9 and 23

Claim 9 is still asserted and states:

> The method of claim 1, further comprising: registering by the client security application, with a network appliance protecting the private network; and receiving, by the client security application, identification information associated with the network appliance.

Patent '034, Claim 9. Claim 23 is still asserted and states:

> The non-transitory computer-readable storage medium of claim 15, wherein the method further comprises: registering with a network appliance protecting the private network; and receiving identification information associated with the network appliance.

Patent '034, Claim 23. Forescout contends that these claims "amount[] to nothing more than sending and receiving information over a network, which is also abstract." Mot. 16. Fortinet, on

the other hand, contends that the invention of Patent '034 lies in a "specific technique" for securing a network embodied in this application:

> This inventive technique lies in discerning a network connection state, or how a device is connected to a private network, and using that in place of a human's judgment as to the needs of the network with respect to specific security functions. [Patent '034's] dependent claims expand on this, describing in more detail how the application discerns this network connection state. Put together, the claims of the '034 Patent address not the mere concept of selecting something based on a condition, but a "specific implementation" of an unconventional technique to overcome technical hurdles. …
> …
> [W]hile Forescout notes that Claim 5 in particular is no longer asserted, that claim merely limits the type of network packet that the application uses to communicate with this network appliance, a DHCP packet, amending the inventive concept of the earlier claims from which it depends. *Id.* at Claim 5. This, however, is just one way for the security application to access the identification information of the network appliance, and one way for it to discern network connection state. All of this is on a backdrop of how this network connection state is integrated into the practical application of securing the private network as a whole, by ensuring that the network is comprised entirely of self-securing devices by virtue of the client security application that is installed on them. Claims 9 and 23 address this aspect as well, requiring the device to register with the appliance, confirming that the devices on the network are running the security application, enabling the entire network to be secured, and providing a variant of the technique for discerning the network connection state. *Id.* at Claims 9, 23. The presence of the security application throughout the devices on the network changes the nature of the network, like how independent cells in an organism act to form more than the sum of their parts.

Opp'n 16-18. As with Claim 4, Claims 9 and 23 appears to limit the scope of the Patent, and "whether a claim limitation or combination of limitations is well-understood, routine, and conventional is a factual question." *BSG Tech LLC v. Buyseasons, Inc.*, 899 F.3d 1281, 1289 (Fed. Cir. 2018). The Court again defers its ruling on this matter until expert testimony can shed light on whether this patent is generic and/or is a technological improvement. Forescout's motion for judgment on the pleadings is thus DENIED with respect to Claims 4, 9, and 23.

3. Patent '421

Patent '421 is titled: "Security Information and Event Management." Patent '421 claims "[s]ystems and methods . . . for conducting work flows by [a Security Information and Event Management ("SIEM")] device to carry out a complex task automatically." Patent '421, Abstract.

Fortinet asserts Claims 5, 8, 9, 18, and 22. *See* Mot. 19. In the Court's motion to dismiss the FAC Order, it provided an overview of the specification:

> According to the patent's specification, contemporary computer networks "may comprise hundreds of . . . devices located in different places, including multiple security devices deployed to protect the network from attacks." Compl. ¶ 39 (citing '421 Patent at 1:21-25). As part of these networks, SIEM devices "may be deployed to aggregate results of tasks performed by the various security devices on a network and alert network administrators" in event of a security breach. *Id.* (citing '421 Patent at 1:30-35). But "problems arise in that the tasks conducted by these disparate security devices are independent," and so may involve "different parameters" and "different configurations depending on the device . . . and its manufacturer."[7] *Id.* (citing '421 Patent at 1:35-36). There was thus "a need for improved SIEM devices that may schedule multiple complex tasks of various security devices to achieve comprehensive management of multiple security devices." *Id.* (citing '421 Patent at 1:43-55). The '421 Patent allegedly solved this problem "in a non-conventional way by having the SIEM configured to allow users [1] to create a work flow that includes multiple security tasks to be performed by one or more security devices, [2] performing these tasks, and [3] collecting the results of these tasks after they are performed." *Id.* (citing '421 Patent at 1:50-60, 18:17-42) (bracketed numbers added). As with the '034 Patent, the Amended Complaint asserts that "[t]he claims of the '421 Patent include inventive concepts" and that "the ordered combination of the recited limitations is not generic and was neither routine nor conventional at the time of invention." *Id.*

Mot. to Dismiss FAC Order at 21, Docket No. 94. The only claim term the Court construed for Patent '421 is the "SIEM" device/system, which the Court construed in terms of its function as a "device/system that identifies and manages security threats by collecting and analyzing logs of security events." Claim Construction Order at 56, Docket No. 174.

a. *Alice* Step One

In the Court's motion to dismiss the FAC Order, it stated:

> The Court again conducts the step-one inquiry in light of the Federal Circuit's forgiving standard for subject-matter eligibility, as articulated in *CardioNet* and *Visual Memory*.
>
> To start, the language of Claim 1 of the '421 Patent is again abstract. The claim "on its face" involves three straightforward steps

[7] At the motion to dismiss hearing, Fortinet offered, as a simple example of the problem the '421 Patent was designed to solve, the need to "make Apple and Windows machines work on the same network." Hearing Tr. at 30, Docket No. 79.

performed by a SIEM device: (1) "creating . . . a work flow" that includes "security tasks" performed by other "security devices" on a computer network, (2) "starting . . . the work flow . . . by scheduling" the security devices "to perform" the security tasks, and (3) "collecting . . . results" of the security tasks after the security devices perform those tasks. *See* '421 Patent at Clm. 1; *see also Am. Axle*, 967 F.3d at 1294, 1298 (focusing on "the face of the claim"). Whether or not the abstract idea to which the method is directed is merely "organizing and monitoring the completion of tasks," as Forescout suggests, Claim 1 *is* written in functional terms and lacks the kind of specific "limiting detail that confines the claim to a particular solution to an identified problem." *See Affinity Labs*, 838 F.3d at 1269; *cf. Am. Axle*, 967 F.3d at 1298 (stating that an invention may successfully incorporate ineligible subject matter where it provides "a specific and detailed series of steps . . . that limit[] the possibility of preempting the [ineligible subject matter] itself").

Additionally, Forescout's analogy between the three-step process of Claim 1 and the travel-agent example in *Yodlee* is revealing, suggesting that the conversion of work flows in Claim 1 "into specific tasks [monitored] by a specialized [actor] coordinating with a variety of [other actors], and then executing those tasks," closely resembles longstanding analog versions of work flow execution and data collection. *See* Reply at 6. This resemblance weighs against finding Claim 1 patent-eligible, as limiting otherwise abstract "claims to a particular field of invention"—*e.g.,* network security—"does not move the claims out of the realm of abstract ideas." *See SAP*, 898 F.3d at 1169; *see also Credit Acceptance Corp. v. Westlake Servs.*, 859 F.3d 1044, 1055 (Fed. Cir. 2017) (stating that "mere automation of manual processes using generic computers does not constitute a patentable improvement in computer technology").

As with the '034 Patent, however, Fortinet raises colorable arguments in favor of finding the '421 Patent non-abstract at step one. Fortinet notes, first, the greater degree of technological specificity contained in some of the patent's dependent claims. For example, Claim 11 derives from Claim 1 but limits the aforementioned workflow to "a website automatic discovery work flow" and the aforementioned security tasks to "a service discovery, a test Hypertext Transfer Protocol (HTTP) service and a website scan." '421 Patent at Clm. 11.[8] And Claim 13, which also depends from Claim 1, confines the work flow to "a closed-loop security event processing work flow," which in turn "comprises event collecting, leakage verification and emergency response processing." *Id*. at Clm. 13.[9] This level of computer-oriented

---

[8] Claim 11 (which is no longer asserted):
The method of claim 1, wherein the work flow comprises a website automatic discovery work flow and the plurality of security tasks comprise a service discovery, a test Hypertext Transfer Protocol (HTTP) service and a website scan.

[9] Claim 13 (which is no longer asserted):
The method of claim 1, wherein the work flow comprises a closed-loop security

> detail suggests that the '421 Patent—at least in its dependent claims—may be "understood as being necessarily rooted in computer technology in order to solve a specific problem in the realm of computer networks." *See SRI Int'l*, 930 F.3d at 1303.
>
> Fortinet also looks to the specification, which asserts that the specialized SIEM device "presents significant advancements over the prior art." Opp'n at 9. The specification states that earlier SIEM devices could perform many of the tasks claimed by the '421 Patent but that they were hindered by the "different parameters" of "security devices from different manufacturers" and could not transfer the results of one security task to another. '421 Patent at 1:30-43. "Thus, there is a need," the specification concluded, "for improved SIEM devices that may schedule multiple tasks of various security devices to automatically achieve comprehensive management." *Id.* at 1:43-46. And in one preferred embodiment of the invention, the SIEM device schedules a work flow in which the constituent security tasks are "sequentially or concurrently executed by multiple security devices despite the security devices being from different manufacturers and/or having different parameters or formats for conducting the tasks." *Id.* at 12:57-61. The '421 Patent's specification therefore "identifies a number of advantages gained by the elements recited in the claimed" invention, and the Court must "accept those statements as true and consider them important" in conducting the step-one inquiry. *See CardioNet*, 955 F.3d at 1369-70.
>
> The specification also mitigates concerns that the '421 Patent is merely a "black box," *see Dropbox*, 815 Fed. Appx. at 533, as it contains lengthy explanations about how the invention's preferred embodiments function. The discussion of Figure 2, for example, runs from the middle of column 6 to the top of column 12, and identifies such specific components as a "device adapter layer," "a WAF," "an IPS/IDS," and "a vulnerability scanner." '421 Patent at 11:62-65. This level of detail in identifying the embodiment's hardware components arguably suggests that the patent provides specific guidance on how it operates and achieves its intended result. On the other hand, it is not clear that this type of specificity actually provides "a specific and detailed series of steps" for performing the claimed method sufficient to satisfy step one. *See Am. Axle*, 967 F.3d at 1298. As noted above with respect to the '034 Patent, that determination would benefit from further developments in the case, such as claim construction and expert testimony.

Mot. to Dismiss FAC Order at 23-25, Docket No. 94.

Forescout argues that this patent is abstract and its abstract idea "is generating tasks based on rules to be completed upon the occurrence of an event" which is a longstanding human activity.

---

event processing work flow and the closed-loop security event processing work flow comprises event collecting, leakage verification and emergency response processing.

Mot. 21; *see also Accenture Glob. Servs., GmbH v. Guidewire Software, Inc.*, 728 F.3d 1336, 1344 (Fed. Cir. 2013) (holding, at summary judgment, a claim which purports to determine which tasks needs to be accomplished and assigns tasks to individuals via a database is abstract where the "claims offer no meaningful limitations" besides "a database of tasks."). Fortinet counters, stating that Patent '421 solves a technological problem: executing a security event with different devices from different manufacturers across a network. *See* Patent '421, col. 1:41-46.

b. *Alice* Step Two

In the Court's prior motion to dismiss the FAC Order, it stated:

> [I]f the Court were to find the '421 Patent directed to an abstract idea at step one, it would once more have difficulty concluding, on a motion to dismiss, that the patent lacks an inventive concept at step two. Fortinet argues, for instance, that the '421 Patent's "specialized SIEM device" was "neither well-understood, routine, nor conventional" in the prior art, as it achieved novel benefits by scheduling and executing security tasks automatically and comprehensively. *See* Opp'n at 15-16 (citing, *e.g.*, '421 Patent at 1:37-46). Fortinet further contends that even if the ordered combination of Claim 1's elements was generic, routine, or conventional, the dependent claims' elements are not. Claims 2 and 13, for example, "introduce additional elements into [the patent's] ordered combination, including the ability to create template work flows" and "the use of a closed-loop security event processing work flow." *Id.* at 16 (citing '421 Patent at Clms. 2 and 13).[10] As Fortinet again emphasizes, "the question of whether the recited steps and features constitute an inventive concept is a fact question that must be decided in Fortinet's favor at th[e] motion to dismiss stage." *Id*. (citing *Berkheimer*, 881 F.3d at 1368). Fortinet also suggests, not unreasonably, that claim construction may be expected to focus the parties' dispute, especially "given, for example, Forescout's sweeping interpretation of the claim term 'security tasks.'" *Id*.

---

[10] Claim 2 (which is no longer asserted):
The method of claim 1, further comprising
Creating a work flow template that defines a complex function and a plurality of abstract security tasks that are needed for performing the complex function; and

Deriving a work flow instance for a security device of the one or more security devices that is designated to conduct the work flow from the work flow template.

Claim 13 (which is no longer asserted):
The method of claim 1, wherein the work flow comprises a closed-loop security event processing work flow and the closed-loop security event processing work flow comprises event collecting, leakage verification and emergency response processing.

> The Court therefore declines to hold, at this stage of the litigation, that the '421 Patent claims ineligible subject matter. It notes, however, that it remains doubtful of the patent's ultimate validity on § 101 grounds, and that Fortinet will face a higher bar in demonstrating as much as the case progresses.

Mot. to Dismiss FAC Order at 25-26, Docket No. 94.

c. Claims 5 and 18

Claims 5 and 18 are still asserted, but relate to Claims 1, 4, and 15, which are no longer asserted. Independent Claim 1, which is not asserted, states:

> A method comprising:
>
> Creating, by a security information and event management (SIEM) device associated with a private network, a work flow, said work flow including information defining a plurality of security tasks that are to be performed by one or more security devices associated with the private network and managed by the SIEM device, wherein the plurality of security tasks include operations that are intended to protect the private network against attacks;
>
> Starting, by the SIEM device, the work flow by scheduling the one or more security devices to perform the plurality of security tasks defined in the work flow; and
>
> Collecting, by the SIEM device, results of the plurality of security tasks after they are performed by the one or more security devices.

Patent '421, Claim 1. Dependent Claim 4, which is no longer asserted, recites:

> The method of claim 1, wherein the plurality of security tasks of the work flow are performed serially.

Patent '421, Claim 4. Dependent Claim 5, which is still asserted, requires:

> The method of claim 4, further comprising determining if a security task of the plurality of security tasks in the work flow should be performed based on the results of one or more previous security tasks of the plurality of security tasks of the work flow.

Patent '421, Claim 5. Independent Claim 15 is no longer asserted. It states:

> A security information and event management (SIEM) system comprising:
> Non-transitory storage device having embodied therein instructions representing a security application; and
> One or more processors coupled to the non-transitory storage device and operable to execute the security application to perform a method comprising:
> Creating a work flow, said work flow including information defining a plurality of security tasks that are to be performed by one or more security devices associated with a private network and managed by the SIEM system, wherein the

> plurality of security tasks include operations that are intended to protect the private network against attacks;
>
> Starting the work flow by scheduling the one or more security devices to perform the plurality of security tasks defined in the work flow; and
>
> Collecting results of the plurality of security tasks after they are performed by the one or more security devices.

Patent '421, Claim 15. Dependent Claim 18 is still asserted and recites:

> The SIEM system of claim 15, wherein the plurality of security tasks of the work flow are performed serially.

Patent '421, Claim 18.

Forescout argues that "deciding to perform a task based on a previous task's results or performing multiple tasks serially are mental steps, not improvements to computer functionality." Mot. at 22. It contends these claims are similar to the Court's travel-agent example, where a travel agent performs tasks based on the results of previous tasks—contacting third parties, researching routes, reviews, customer preferences—and does these tasks serially. *See* Mot. to Dismiss FAC Order at 22, Docket No. 94. The Court had cited a prior decision that found that "individuals have long identified sub-tasks of a more complex undertaking, managed the completion of such sub-tasks, and conveyed the results to the requesting party." *Id*. at 22 (quoting *Yodlee, Inc. v. Plaid Techs. Inc.*, 2016 WL 2982503, at *17 (D. Del. 2016)).

Fortinet responds arguing that this patent solves a technological problem:

> [T]he issue of 'security devices from different manufacturers' requiring 'different parameters' to function, giving rise to the need 'for improved SIEM devices that may schedule multiple tasks of various security devices to automatically achieve comprehensive management. '421 Patent at 1:41-46. It solves this problem by proposing an improved SIEM device that can execute flexible work flows for scheduling tasks. Forescout mistakes this flexibility, a crucial feature of the patent, for abstractness.

Opp'n at 19.

Here, at *Alice* step one, Claims 5 and 18 are abstract on their face—Claim 5 alludes to performing tasks based on information imported from other tasks or based on learning from prior results a way to perform future tasks. Claim 18 simply states that tasks will be performed in a sequential order. Neither of these claims provide computer-oriented detail as Claim 13 did (which

confined the work flow to "a closed-loop security event processing work flow," which in turn "comprises event collecting, leakage verification and emergency response processing," Claim 13.). Fortinet submits that Claim 5 indicates "the aspects of allowing the results of previous tasks to influence future tasks." Opp'n at 22. These claims' processes "generate tasks based on rules to be completed upon the occurrence of an event," which is abstract. *Accenture Glob. Servs., GmbH v. Guidewire Software, Inc.*, 728 F.3d 1336, 1344 (Fed. Cir. 2013).[11]

At *Alice* step two, Forescout argues that the nonconventional claims (claims 2 and 13) have been dropped and claim construction did not limit the meaning of the terms in a substantive way. Mot. at 24. There is nothing unconventional in the remaining asserted claims besides the "three straightforward steps" (creating and starting the work flow and collecting the results of the tasks) that the Court found "abstract." Mot. to Dismiss FAC Order at 23, Docket No. 94. Conversely, Fortinet states that "the work flows of the claims are more than simply the idea of organizing and monitoring tasks, but a specific technique to 'solve a technological problem arising in computer networks,' the incompatibility between security devices on a network." Opp'n at 24 (citing *SRI Int'l, Inc. v. Cisco Systems, Inc.*, 930 F.3d 1295, 1303 (Fed. Cir. 2019)).

Again, at *Alice* step two, the Court should assess:

> [W]e "search for an 'inventive concept' … that is 'sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.'" *Alice*, 134 S.Ct. at 2355 (internal quotation marks omitted) (quoting *Mayo*, 566 U.s. at 72-73). After identifying an ineligible concept at step one, we ask at step two "[w]hat else is there in the claims before us?" *Mayo*, 566 U.S. at 78.
>
> It has been clear since *Alice* that a claimed invention's use of the ineligible concept to which it is directed cannot supply the inventive concept that renders the invention "significantly more" than that ineligible concept.
> …
> If a claim's only "inventive concept" is the application of an abstract

[11] Forescout asserts that, because the specification "admits" that the "steps may be performed by a combination of hardware, software, firmware and/or by human operators," that the patent must be directed to an abstract idea that could be completed via human activity. Mot. at 21. Aside from this cited language, the specification of the patent does state than an administrator can add a website to the work flow or indicate their desire to be notified of an alarm, but the specification otherwise provides complex processes which clearly would be completed by a computer, not a human being.

> idea using conventional and well-understood techniques, the claim has not been transformed into a patent-eligible application of an abstract idea.

BSG, 899 F.3d at 1290-91. Thus, for the remaining asserted claims, they need to add "significantly more" to the patent than the three basic steps of a SIEM device, which the Court found to be abstract at *Alice* step one. If the remaining asserted claims "contain limitations directed to the arguably unconventional inventive concept described in the specification," *Berkheimer*, 881 F.3d 1370, then they should survive the *Alice* test at least at this juncture.

For Claims 5 and 18, Fortinet states that the asserted dependent claims add to the concept of a flexible work flow:

> Claims 5 and 18 add the aspect of serial and parallel execution, or various ways in which the SIEM device can schedule tasks. '421 Pat. at Claims 5, 18. Similarly, Claim 5 captures one key benefit of the invention in allowing the results of previous tasks to influence future tasks. *Id.* at Claim 5.

Opp'n at 24. Indeed, Claims 5 and 18 likely correlate with the following language in the specification:

> Work flow manager is used for configuring work flows that can be executed by SIEM device to carry out complex tasks. A work flow defines a work flow task that contains a group of tasks that may be sequentially or concurrently conducted by one or more security devices so that a complex function may be accomplished automatically by SIEM device. The results of a previous tasks in the work flow may be used to trigger the next task and the results may be transferred as parameters to the next task.

Patent '421, col. 8:17-25.

In the Court's prior Order, it discussed Claims 2 and 13 as essentially saving Patent '421 from ineligibility at *Alice* step two. However, those claims are no longer asserted. In the Court's prior Order it stated:

> Claims 2 and 13, for example, "introduce additional elements into [the patent's] ordered combination, including the ability to create template work flows" and "the use of a closed-loop security event processing work flow." *Id.* at 16 (citing '421 Patent at Clms. 2 and 13). As Fortinet again emphasizes, "the question of whether the recited steps and features constitute an inventive concept is a fact question that must be decided in Fortinet's favor at th[e] motion to dismiss stage." *Id.* (citing *Berkheimer*, 881 F.3d at 1368).

Mot. to Dismiss FAC Order at 25-26, Docket No. 94. Claim 2 adds particularity to Claim 1,

stating "deriving a work flow instance for a security device of the one or more security devices that is designated to conduct the work flow from the work flow template." Patent '421, Claim 2.

Here, Claims 5 and 18 recite steps that are more conventional than Claims 2 and 13. Notably, at *Alice* step one, the Court above found Claim 5 abstract; "it alludes to performing tasks based on information imported from other tasks or based on learning from prior results a way to perform future tasks." At *Alice* step two, a claim needs to add "significantly more" to the abstract concept found at step one. *BSG*, 899 F.3d at 1290-91. The Federal Circuit has emphasized the need for an inventive concept at step two.

In *Elec. Power Group*, the Federal Circuit found a company's patents ineligible which described "collecting data from multiple data sources, analyzing the data, and displaying the results." 830 F.3d at 1351. "Though lengthy and numerous, the claims do not go beyond requiring the collection, analysis, and display of available information in a particular field, stating those functions in general terms, without limiting them to technical means for performing the functions that are arguably an advance over conventional computer and network technology." *Id.* Representative Claim 12 recites:

> A method of detecting events … and automatically analyzing the events … the method comprising:
>
> *Receiving a plurality of data streams* . . .;
>
> *Receiving data from other power system data sources*, . . .;
>
> *Detecting and analyzing events in real-time from the plurality of data streams* from the wide area based on at least one of limits, sensitivities and rates of change for one or more measurements from the data streams and dynamic stability metrics derived from analysis of the measurements from the data streams. . .;
>
> *Displaying the event analysis results and diagnoses of events and associated ones of the metrics from different categories of data and the derived metrics in visuals, tables, charts, or combinations thereof, the data comprising at least one of monitoring data, tracking data, historical data, prediction data, and summary data*;
>
> Displaying concurrent visualization of measurements from the data streams and the dynamic stability metrics directed to the wide area of the interconnected electric power grid;
>
> *Accumulating and updating the measurements from the data streams* and the dynamic stability metrics, grid data, and non-grid data in

> real time as to wide area and local area portions of the interconnected electric power grid; and
>
> *Deriving a composite indicator of reliability that is an indicator of power grid vulnerability and is derived from a combination of one or more real time measurements or computations of measurements from the data streams and the dynamic stability metrics* covering the wide area as well as non-power grid data received from the non-grid data source.

Id. at 1352 (emphasis added). At step one, the court stated that "collecting information, including when limited to particular content (which does not change its character as information), [is] within the realm of abstract ideas." *Id*. at 1353. At step two, the court stated that the claim "merely select[s] information, by content or source, for collection, analysis, and display" and "do[es] not even require a new source or type of information, or new techniques for analyzing it." *Id*. at 1355. There are no "requirements for how the desired result is achieved." *Id*. (emphasis in original). The court contrasted the case to *BASCOM*, 827 F.3d at 1350, where, at pleading stage, the Federal Circuit found an inventive concept in "the installation of a filtering tool at a specific location, remote from the end-users, with customizable filtering features specific to each end user" which exemplified an "arguably inventive distribution of functionality within a network." *Id*. at 1355-56.

In *Affinity Labs of Texas, LLC v. Amazon.com, Inc.*, the Federal Circuit considered a patent which specified selection of an advertisement "for delivery to the user of a portable device based on at least one piece of demographic information about the user." 838 F.3d 1266, 1267 (Fed Cir. 2016). The court addressed one representative claim, which was "directed to a network-based media system with a customized user interface, in which the system delivers streaming content from a network-based resource upon demand to a handheld wireless electronic device having a graphical user interface." *Id*. The claim language specified that "the network based delivery resource configured to respond to the request by retrieving the portion from an appropriate network location and streaming a representation of the portion to the handheld wireless device." *Id*. At step one, the concept of "delivering user-selected media content to portable devices" was found to be abstract. *Id*. at 1269. At step two, the court found the patent to be ineligible, stating that the features described were "generic." *Id*. at 1271. The only limitation was that there was a "customized user interface" which could be customized "'in a plurality of ways' by allowing users

to select and receive 'on-demand customized audio information.'" *Id*. at 1271-72. "Basic user customization features" were insufficient to "alter the abstract nature of the claims." *Id*. at 1272.

Here, Claim 5 does not say anything about *how* it transforms prior results into future results; it does not "constitute a concrete application of the abstract idea." *Id.* at 1272. The specification does not add precision or definition; it merely specifies that tasks will be performed based on prior tasks, which is exactly what the Court found to be abstract at step one. As in *Affinity Labs*, "[t]he features set forth in the claims are described and claimed generically rather than with the specificity necessary to show how those components provide a concrete solution to the problem addressed by the patent." *Id*. at 1271. Claim 5 merely describes a process of "configur[ing] to respond to [a] request by retrieving [a] portion from [a location]," *id*. at 1267; it says nothing about how the process configures the data. It describes no novel or unconventional process. As in *Elec. Power Group* and *Affinity Labs*, Claim 5 is non-inventive and patent-ineligible.

Claim 18 merely adds the aspect of serial and parallel execution. *See* Patent '421, Claim 18 ("wherein the plurality of security tasks of the work flow are performed serially"); Opp'n at 24. Fortinet has failed to demonstrate this is inventive—Claim 18 merely suggests a well-known order of events (serial as opposed to parallel). The Federal Circuit has repeatedly held that claims which generically illustrate a process of "merely selecting information, by content or source, for collection, analysis, and display" are ineligible, and Claims 5 and 18 do not do more than that. *Elec. Power Group*, 830 F.3d at 1355. These claims do not employ any unconventional or inventive step that materially adds to the abstract steps in Claim 1. Thus, Claim 18 is also patent-ineligible.

d. Claims 8, 9 and 22

Claims 8 and 22 are substantially similar and are still asserted. Claim 8 recites:

> The method of claim 1, wherein said collecting, by the SIEM device, results of the plurality of security tasks further comprises normalizing the results.

Patent '421, Claim 8. Claim 9 is still asserted and recites:

> The method of claim 1, further comprising: performing asset

> correlation to the results of the plurality of security tasks; reporting the results of the plurality of security tasks if they are correlated to core network assets.

Patent '421, Claim 9.

At *Alice* step one, Forescout asserts that the "work flows" are created by human users, so "there is nothing in the claims themselves that foreclose them from being performed by a human, mentally or with pen and paper." Mot. 21; *Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1318 (Fed. Cir. 2016). Conversely, Fortinet submits that the patent "propos[es] an improved SIEM device that can execute flexible work flows for scheduling tasks" and that the flexibility is a crucial feature of the patent. Opp'n at 19. It states that the specification explains that a work flow would compromise "logical conditions" which "may be defined to determine if a subsequent task in a work flow should be conducted." Opp'n 21; *see also* Patent '421, col. 2:42-44.

Additionally, Forescout contends that these asserted claims "merely recite data-processing and reporting steps that are entirely abstract: 'normalizing the results' (Claims 8, 22), 'performing asset correlation,' and 'reporting the results' (Claim 9). These generic, functionally recited steps fail to recite a technological improvement as a matter of law." Mot. at 23; *see also Elec. Power Grp.*, 830 F.3d at 1353-54 (the claims were abstract because they "gather[ed] and analyz[ed] information of a specified content, then display[ed] the results" which did not show "any particular assertedly inventive technology for performing those functions."); *FairWarning IP, LLC v. Iatric Sys., Inc.,* No. 8:14-cv-2685-T-23MAP, 2015 WL 3883958 at *4 (M.D. Fla. June 24, 2015), *aff'd*, 839 F.3d 1089 (Fed. Cir. 2016) (the patent collected information, analyzed the information according to one of several rules, and provided a binary yes/no determination and the specification did not elaborate upon the system's "improvement" in the field).

However, the Court has previously held: "the '421 Patent's specification therefore "identifies a number of advantages gained by the elements recited in the claimed" invention, and the Court must "accept those statements as true and consider them important" in conducting the step-one inquiry. *See CardioNet*, 955 F.3d at 1369-70." Mot. to Dismiss FAC Order at 25, Docket No. 94. Indeed, the specification provides greater detail with respect to these two claims.

Claim 8 correlates to the following language in the specification:

> Device adapter layer represents interfacing modules that connect SIEM device and security devices of the network managed by SIEM device for collecting security events from the security devices. … the adapters allow SIEM device to schedule different security devices to conduct designated tasks and receive security events and results of tasks in uniform formats. … Collectors are used for collecting original security events from security devices. These original security events from different security devices may contain different contents in different formats. The original security events may be sent to normalization and for normalizing. After normalization, the information that is useful for correlation in the original security events may be retained and saved in a unified format. It will be easier for correlation engines to correlate events from different sources after the original events are normalized.

Patent '421, col. 11:19-44; *see also* Opp'n at 23. Further, Claim 9 appears to correlate to the following language in the specification:

> Asset manager is used for managing asset attributes of networks managed by SIEM device. Asset manager may create and update one or more asset tables in data storage to register all or core assets of the network(s). Each of the assets or core assets may be assigned an asset value. A risk level of an event may be set and adjusted based on an asset value and/or other attributes of the target of the event in the network. If the target of the vent is a core asset of the network, the calculated risk level of the event may result in a higher value relative to a calculated risk level of a non-core asset. For example, a web server providing the most important web application for a company would be considered a core asset of the whole network and would typically be assigned a high asset value. When an attack is targeting this web server, the determined risk level of this attack is high and therefore an alarm is more likely to be generated by SIEM device. On the other hand, a client PC within the network would typically be considered a non-core asset of the network or may not even be present in the asset list of the network. When an attack is targeting this client PC, the determined risk level is low and therefore no alarm is sent to the administrators.

Patent '421, col. 7:8-29.

Even if these claims are directed to an abstract idea, at *Alice* step two the Court would "have difficulty concluding, on a motion [for judgment on the pleadings], that the patent lacks an inventive concept at step two." Claim Construction Order at 25, Docket No. 174. Though the claim construction added a definition of SIEM, the claim construction did not limit the claims' ability to add nuance to the definition of a SIEM device, as Forescout seemingly suggests. Instead, Fortinet argus that Patent '421 provides for an "unconventional modification of an SIEM

device to allow it to execute complex work flows involving multiple devices from multiple vendors." Opp'n at 22. Fortinet argues that Patent '421 solves the following technological problem:

> In its earlier opinion, the Court noted that, "in one preferred embodiment of the invention, the SIEM device schedules a work flow in which the constituent security tasks are 'sequentially or concurrently executed by multiple security devices despite the security devices being from different manufacturers and/or having different parameters or formats for conducting the tasks.'" Dkt. 94 at 24 (quoting '421 Pat. at 12:57-61). This aspect of sequential (serial) and concurrent (parallel) execution is present in asserted Claims 5 and 18.
> …
> Without the improved claimed device, "tasks that can be conducted by security devices of the network are independent and results of such tasks cannot be transferred to another task, as tasks required "different parameters" when conducted by "different security devices" or even the same security devices "from different manufacturers."
> …
> Claim 8's introduction of normalization as a means of ensuring that results are usable between tasks adds an aspect of how these benefits can concretely be achieved. *Id*. at Claim 8. Moreover, the asset correlation engine described in the specification is addressed in Claim 9, and provides another practical application of these work flows: the ability to correlate events and tasks with specific hardware on a network. *See* '421 Pat. At 9:65-10:11, Claim 9. Together, these dependent claims crystalize the inventive concept present in the independent claims, and at the very least raise fact issues as to the unconventionality of these further aspects of the claims.

Id. at 21-22, 24. Accordingly, it appears that Claims 8 and 22 add that the SIEM device collects and normalizes the results of many security tasks, which aids the process of correlate[ing] events from different sources. This claim is similar to Claim 2, which "introduce[s] additional elements into the patent's ordered combination…" Mot. to Dismiss FAC Order at 25, Docket No. 94. As the Court stated in its prior Order, "the question of whether the recited steps and features constitute an inventive concept is a fact question that must be decided in Fortinet's favor at th[e] motion to dismiss stage." *Id*. (citing *Berkheimer*, 881 F.3d at 1368).

Thus, Forescout's motion for judgment on the pleadings is DENIED with respect to Claims 8, 9, and 22.

V. CONCLUSION

The Court finds that Patents '662, '034, and '421 are still patent-eligible. However,

Claims 5 and 13 of Patent '662 and Claims 5 and 18 of Patent '421 are patent-ineligible. The Court reasserts its skepticism of the ultimate eligibility of some of these claims, but at this time, the Court cannot make this determination without further factual development and expert testimony.

This order disposes of Docket No. 208.

IT IS SO ORDERED.

Dated: April 15, 2024

EDWARD M. CHEN
United States District Judge